

Symmetries of finite Heisenberg groups for multipartite systems

M. Korbelař¹ and J. Tolar²

¹ Department of Mathematics and Statistics
Faculty of Science, Masaryk University
Kotlářská 2, 611 37 Brno, Czech Republic

² Department of Physics
Faculty of Nuclear Sciences and Physical Engineering
Czech Technical University in Prague
Břehová 7, 115 19 Prague 1, Czech Republic

E-mail: miroslav.korbelar@gmail.com, jiri.tolar@fjfi.cvut.cz

PACS numbers: 03.65.-w, 03.65.Aa, 03.65.Fd, 02.10.Hh, 02.20.-a, 03.67.-a

Abstract. A composite quantum system comprising a finite number k of subsystems which are described with position and momentum variables in \mathbb{Z}_{n_i} , $i = 1, \dots, k$, is considered. Its Hilbert space is given by a k -fold tensor product of Hilbert spaces of dimensions n_1, \dots, n_k . Symmetry group of the respective finite Heisenberg group is given by the quotient group of certain normalizer. This paper extends our previous investigation of bipartite quantum systems to arbitrary multipartite systems of the above type. It provides detailed description of the normalizers and the corresponding symmetry groups. The new class of symmetry groups represents a very specific generalization of symplectic groups over modular rings. As an application, a new proof of existence of the maximal set of mutually unbiased bases in Hilbert spaces of prime power dimensions is provided.

1. Introduction

The Heisenberg Lie algebra and the Heisenberg-Weyl group lie at the heart of quantum mechanics [1]. Therefore their symmetries induced by unitary automorphisms play very important role in quantum kinematics as well as quantum dynamics. The growing interest in quantum communication science has pushed the study of quantum systems with finite-dimensional Hilbert spaces to the forefront, both single systems and composite systems. For them the finite Heisenberg groups provide the basic quantum observables. It is then clear that the symmetries of finite Heisenberg groups uncover deeper structure of finite-dimensional quantum mechanics.

Our continuing interest in finite-dimensional quantum mechanics goes back to the paper [2] where finite-dimensional quantum mechanics was developed as quantum mechanics on configuration spaces given by finite sets equipped with the structure of a finite Abelian group. In our recent paper [3] detailed characterization was given of the symmetry groups of finite Heisenberg groups for composite quantum systems consisting of two subsystems with arbitrary dimensions n, m . In this contribution these results for bipartite systems are extended to the general finitely composed systems consisting of an arbitrary number k of subsystems with arbitrary dimensions n_1, \dots, n_k . Their Hilbert spaces are given by k -fold tensor products of Hilbert spaces of dimensions n_1, \dots, n_k .

In the course of work it turned out that — even if the idea of the present paper is similar to [3] — intermediate steps could not be taken over literally from [3], but had to be carefully developed in the general multipartite situation. Preliminary results were given in [4].

The exposition starts with introductory material on finite-dimensional quantum mechanics in section 2. In section 3 the group $\text{Sp}_{[n_1, \dots, n_k]}$ is introduced. Its further properties are given in section 4. The proof that $\text{Sp}_{[n_1, \dots, n_k]}$ is indeed the symmetry group is contained in section 5, theorem 5.9. The reader will see that the new family of finite groups deserves the chosen notation because they generalize finite symplectic groups over modular rings [5].

A special subclass $\text{Sp}_{2k}(\mathbb{Z}_p)$ of our family of symmetry groups is applied in section 6 to an alternative proof of existence of the maximal set of mutually unbiased bases in Hilbert spaces of prime power dimensions p^k [6, 7]. We remind that previous group theoretical construction of mutually unbiased bases presented in [8] was based on the symmetry groups $\text{SL}_2(\mathbb{Z}_p)$ of the finite Heisenberg groups for Hilbert spaces of prime dimensions p .

2. Finite-dimensional quantum mechanics

For reader's convenience we very briefly repeat the basic notions of finite-dimensional quantum mechanics (FDQM) [9, 10] for a single-component system with the Hilbert space $\ell^2(\mathbb{Z}_n)$ of arbitrary dimension $n \in \mathbb{N}$. In this case the cyclic group \mathbb{Z}_n serves as the underlying configuration space.

We follow the notation of [3], where further details can be found. For a given $n \in \mathbb{N}$ we set

$$\omega_n := e^{2\pi i/n} \in \mathbb{C}.$$

Let Q_n and P_n denote the *generalized Pauli matrices* of order n ,

$$Q_n := \text{diag}(1, \omega_n, \omega_n^2, \dots, \omega_n^{n-1}) \in \text{GL}_n(\mathbb{C})$$

and

$$P_n \in \text{GL}_n(\mathbb{C}), \quad \text{where} \quad (P_n)_{i,j} := \delta_{i,j-1}, \quad i, j \in \mathbb{Z}_n.$$

They belong to the group $\text{U}_n(\mathbb{C})$ of $n \times n$ unitary matrices in $\ell^2(\mathbb{Z}_n)$. Let I_n denote the $n \times n$ unit matrix. The subgroup of unitary matrices in $\text{GL}_n(\mathbb{C})$ generated by Q_n and P_n ,

$$\Pi_n := \{\omega_n^j Q_n^k P_n^l | j, k, l \in \{0, 1, \dots, n-1\}\}$$

is called the *finite Heisenberg group*. Recall that the order of Π_n is n^3 , its center is $Z(\Pi_n) = \{\omega_n^j I_n | j \in \{0, 1, \dots, n-1\}\}$ and

$$P_n Q_n = \omega_n Q_n P_n. \tag{1}$$

For $M \in \text{GL}_n(\mathbb{C})$ let $\text{Ad}_M \in \text{Int}(\text{GL}_n(\mathbb{C}))$ be the *inner automorphism* of the group $\text{GL}_n(\mathbb{C})$ induced by operator $M \in \text{GL}_n(\mathbb{C})$, i.e.

$$\text{Ad}_M(X) = M X M^{-1} \quad \text{for} \quad X \in \text{GL}_n(\mathbb{C}).$$

Definition 2.1. We define \mathcal{P}_n as the group

$$\mathcal{P}_n = \{\text{Ad}_{Q_n^i P_n^j} | (i, j) \in \mathbb{Z}_n \times \mathbb{Z}_n\}.$$

It is an Abelian subgroup of $\text{Int}(\text{GL}_n(\mathbb{C}))$ and is generated by two commuting automorphisms $\text{Ad}_{Q_n}, \text{Ad}_{P_n}$,

$$\mathcal{P}_n = \langle \text{Ad}_{Q_n}, \text{Ad}_{P_n} \rangle.$$

A geometric view is sometimes useful that \mathcal{P}_n is isomorphic to the *quantum phase space* identified with the Abelian group \mathbb{Z}_n^2 [11, 8].

Let us recall the usual properties of the matrix tensor product \otimes . Let $A, A' \in \text{GL}_n(\mathbb{C})$, $B, B' \in \text{GL}_m(\mathbb{C})$ and $\alpha \in \mathbb{C}$. Then:

- (i) $(A \otimes B)(A' \otimes B') = AA' \otimes BB'$.
- (ii) $\alpha(A \otimes B) = (\alpha A) \otimes B = A \otimes (\alpha B)$.
- (iii) $A \otimes B = I_{nm}$ if and only if there is non-zero $\alpha \in \mathbb{C}$ such that $A = \alpha I_n$ and $B = \alpha^{-1} I_m$.

Finally we introduce the main notions for the k -partite situation where the group $\mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}$ (with $n_1, \dots, n_k \in \mathbb{N}$) serves as the configuration space.

Definition 2.2. Let $n_1 \dots n_k = N$. We define

$$\mathcal{P}_{(n_1, \dots, n_k)} = \{\text{Ad}_{M_1 \otimes \cdots \otimes M_k} \mid M_i \in \Pi_{n_i}\} \subseteq \text{Int}(\text{GL}_N(\mathbb{C})).$$

In the following we shall work with generating elements of the finite Heisenberg group $\Pi_{n_1} \otimes \cdots \otimes \Pi_{n_k}$,

$$A_{2i-1} := I_{n_1 \cdots n_{i-1}} \otimes P_{n_i} \otimes I_{n_{i+1} \cdots n_k}, \quad A_{2i} := I_{n_1 \cdots n_{i-1}} \otimes Q_{n_i} \otimes I_{n_{i+1} \cdots n_k}, \quad (2)$$

for $i = 1, \dots, k$ and the corresponding inner automorphisms

$$e_j := \text{Ad}_{A_j} \quad \text{for } j = 1, \dots, 2k.$$

Clearly, $\mathcal{P}_{(n_1, \dots, n_k)}$ is an Abelian group given by the direct product of the groups $\langle e_j \rangle$, where $j = 1, \dots, 2k$.

Lemma 2.3. Let $n_1 \dots n_k = N$. Then $\mathcal{P}_{(n_1, \dots, n_k)}$ is a maximal Abelian subgroup of diagonalizable automorphisms in $\text{Int}(\text{GL}_N(\mathbb{C}))$.

This subgroup has been called a MAD-group [12, 13] and it is the subgroup of $\text{Int}(\text{GL}_N(\mathbb{C}))$ such that its centralizer in $\text{Int}(\text{GL}_N(\mathbb{C}))$ is equal to $\mathcal{P}_{(n_1, \dots, n_k)}$. The proof for the bipartite case was given in [3, 4.3].

3. The symmetry group $\text{Sp}_{[n_1, \dots, n_k]}$

In this section the group $\text{Sp}_{[n_1, \dots, n_k]}$ is defined as a matrix subgroup of $\text{GL}_N(\mathbb{C})$ and its principal properties are proved. It will be constructed in several steps. Through this section and sections 4 and 5 let $n_1, \dots, n_k \in \mathbb{N}$ be fixed numbers and let $M_n(\mathcal{R})$ be the ring of $n \times n$ matrices with entries from the ring \mathcal{R} .

Our construction starts with a set of block matrices:

Definition 3.1. Let $\mathcal{M}_{[n_1, \dots, n_k]}$ be a set consisting of $k \times k$ matrices H composed of 2×2 blocks

$$H_{ij} = \frac{n_i}{\gcd(n_i, n_j)} A_{ij}$$

where $A_{ij} \in M_2(\mathbb{Z}_{n_i})$ for $i, j = 1, \dots, k$, are 2×2 matrices over \mathbb{Z}_{n_i} .

It is useful to take such matrices over \mathbb{Z} ,

$$\mathcal{S}_{[n_1, \dots, n_k]} := \left\{ H \in M_k(M_2(\mathbb{Z})) \mid A_{ij} \in M_2(\mathbb{Z}), H_{ij} = \frac{n_i}{\gcd(n_i, n_j)} A_{ij}, i, j = 1, \dots, k \right\},$$

and, using a special diagonal matrix

$$D := \text{diag}\left(\frac{\text{lcm}(n_1, \dots, n_k)}{n_1} I_2, \dots, \frac{\text{lcm}(n_1, \dots, n_k)}{n_k} I_2\right) \in \mathcal{S}_{[n_1, \dots, n_k]},$$

to define a congruence \equiv on $\mathcal{S}_{[n_1, \dots, n_k]}$:

$$H \equiv G \Leftrightarrow DH \equiv_{\text{lcm}(n_1, \dots, n_k)} DG, \quad \text{where } H, G \in \mathcal{S}_{[n_1, \dots, n_k]}.$$

Further an adjoint $H^* \in \mathcal{S}_{[n_1, \dots, n_k]}$ of $H \in \mathcal{S}_{[n_1, \dots, n_k]}$, $H_{ij} = \frac{n_i}{\gcd(n_i, n_j)} A_{ij}$ is defined by

$$(H^*)_{ij} = \frac{n_i}{\gcd(n_i, n_j)} A_{ji}^T.$$

For convenience we put $\ell := \text{lcm}(n_1, \dots, n_k)$ in this section.

Remark 3.2. The above definitions lead to the following properties of $\mathcal{M}_{[n_1, \dots, n_k]}$:

- (i) Let $d, n, a, b \in \mathbb{Z}$ and $d \mid n$. Then the congruence $\frac{n}{d}a \equiv_n \frac{n}{d}b$ is equivalent to $a \equiv_d b$, i.e. $a \equiv b \pmod{d}$.
- (ii) By (i), we see that $\mathcal{M}_{[n_1, \dots, n_k]} = \mathcal{S}_{[n_1, \dots, n_k]} / \equiv$.
- (iii) Let $i, j, m \in \{1, \dots, k\}$. Then $\frac{n_i}{\gcd(n_i, n_j)} \mid \frac{n_i}{\gcd(n_i, n_m)} \frac{n_m}{\gcd(n_m, n_j)}$.
Indeed, $\gcd(n_m, n_j) \cdot \gcd(n_i, n_m)$ divides $n_m n_i$ and also $n_j n_m$. Hence $\gcd(n_m, n_j) \cdot \gcd(n_i, n_m)$ divides $\gcd(n_m n_i, n_m n_j) = n_m \gcd(n_i, n_j)$ and thus

$$\frac{n_m \gcd(n_i, n_j)}{\gcd(n_i, n_m) \gcd(n_m, n_j)} \in \mathbb{Z}.$$

- (iv) Using (iii) we get that $\mathcal{S}_{[n_1, \dots, n_k]}$ is a subring of $M_k(M_2(\mathbb{Z}))$.
- (v) It is easy to verify that $DH = (H^*)^T D$ for every $H \in \mathcal{S}_{[n_1, \dots, n_k]}$.
- (vi) \equiv is a ring congruence on $\mathcal{S}_{[n_1, \dots, n_k]}$. Thus, by (ii) and (iv), $\mathcal{M}_{[n_1, \dots, n_k]}$ is (with the usual matrix multiplication and addition) a ring.
It is enough to show that $\mathcal{I} := \{H \in \mathcal{S}_{[n_1, \dots, n_k]} \mid H \equiv 0\}$ is an ideal in $\mathcal{S}_{[n_1, \dots, n_k]}$. Let $H, G \in \mathcal{S}_{[n_1, \dots, n_k]}$ and $H \in \mathcal{I}$. Then $DH \equiv_\ell 0$. Hence by (v) we have $D(GH) \equiv_\ell (G^*)^T (DH) \equiv_\ell 0$ and $GH \in \mathcal{I}$. The rest is obvious.
- (vii) $\mathcal{M}_{[n_1, \dots, n_k]}$ has a natural action (via the matrix multiplication) on the quantum phase space $\mathbb{Z}_{n_1}^2 \times \dots \times \mathbb{Z}_{n_k}^2$.
Clearly, $\mathbb{Z}_{n_1}^2 \times \dots \times \mathbb{Z}_{n_k}^2$ can be viewed as \mathbb{Z}^{2k} factorized by the equivalence: $x \equiv y$ if and only if $Dx \equiv_\ell Dy$, where $x, y \in \mathbb{Z}^{2k}$. One needs only to show that $H \equiv G$ and $x \equiv y$ implies $Hx \equiv Gy$ for $H, G \in \mathcal{S}_{[n_1, \dots, n_k]}$ and $x, y \in \mathbb{Z}^{2k}$. Let $DH \equiv_\ell DG$ and $Dx \equiv_\ell Dy$. Then $DHx \equiv_\ell (DG)x \equiv_\ell (G^*)^T (Dx) \equiv_\ell (G^*)^T Dy \equiv_\ell DGY$ and thus $Hx \equiv Gy$.
- (viii) $\mathcal{M}_{[n_1, \dots, n_k]}$ is a finite set of matrices closed under usual matrix multiplication and containing the unit matrix as neutral element, i.e. it is a finite monoid.

Property (vii) can be naturally extended to any endomorphism of the quantum phase space $\mathcal{K} = \mathbb{Z}_{n_1}^2 \times \dots \times \mathbb{Z}_{n_k}^2$:

Proposition 3.3. For every $\alpha \in \text{End}(\mathbb{Z}_{n_1}^2 \times \dots \times \mathbb{Z}_{n_k}^2)$ there is a unique $H \in \mathcal{M}_{[n_1, \dots, n_k]}$ such that $\alpha(x) = Hx$ for every $x \in \mathbb{Z}_{n_1}^2 \times \dots \times \mathbb{Z}_{n_k}^2$. The map

$$\Phi : \text{End}(\mathbb{Z}_{n_1}^2 \times \dots \times \mathbb{Z}_{n_k}^2) \rightarrow \mathcal{M}_{[n_1, \dots, n_k]},$$

where $\Phi(\alpha) := H$ is a ring isomorphism.

Proof. Let $\{f_1, \dots, f_{2k}\}$ be the canonical generating set of $\mathbb{Z}_{n_1}^2 \times \dots \times \mathbb{Z}_{n_k}^2$. For every $\alpha \in \text{End}(\mathbb{Z}_{n_1}^2 \times \dots \times \mathbb{Z}_{n_k}^2)$ there are $h_{ij} \in \mathbb{Z}$ such that $\alpha(f_j) = \sum_{i=1}^{2k} h_{ij} f_i$. The order of f_{2i-1} and f_{2i} is n_i for $i = 1, \dots, k$. Hence we have $1 = \alpha(n_i f_{2i-1}) = \sum_{j=1}^{2k} (n_i h_{j, 2i-1}) f_j$ and $1 = \alpha(n_i f_{2i}) = \sum_{j=1}^{2k} (n_i h_{j, 2i}) f_j$. Thus $n_i h_{2j-1, 2i} \equiv_{n_j} 0 \equiv_{n_j} n_i h_{2j, 2i}$ for every $j = 1, \dots, k$. It follows that $\frac{n_i}{\gcd(n_i, n_j)} h_{2j-1, 2i} \equiv_{n_j / \gcd(n_i, n_j)} 0 \equiv_{n_j / \gcd(n_i, n_j)} \frac{n_i}{\gcd(n_i, n_j)} h_{2j, 2i}$ and $h_{2j-1, 2i}, h_{2j, 2i} \in \frac{n_j}{\gcd(n_i, n_j)} \mathbb{Z}$ for every $j = 1, \dots, k$. Now, consider h_{ij} modulo $[n_i/2]$. Put $H = (h_{ij})_{i,j=1, \dots, 2k} \in \mathcal{M}_{[n_1, \dots, n_k]}$ and the rest is easy. \square

Remark 3.4. Properties of the adjoint operation given below mean that $\mathcal{S}_{[n_1, \dots, n_k]}$ and $\mathcal{M}_{[n_1, \dots, n_k]}$ have the structure of a $*$ -ring:

- (i) Let $H, G \in \mathcal{S}_{[n_1, \dots, n_k]}$. Then $(H^*)^* = H$, $(H + G)^* = H^* + G^*$ and $(HG)^* = G^*H^*$, i.e. the operation $*$ is an involutive ring antihomomorphism.

Let $H_{ij} = \frac{n_i}{\gcd(n_i, n_j)} A_{ij} \in \mathbb{Z}_{n_i}$ and $G_{ij} = \frac{n_i}{\gcd(n_i, n_j)} B_{ij} \in \mathbb{Z}_{n_i}$ for $i, j = 1, \dots, k$. Then

$$\begin{aligned} (G^*H^*)_{ij} &= \sum_{m=1}^k \frac{n_i}{\gcd(n_i, n_m)} \frac{n_m}{\gcd(n_m, n_j)} B_{mi}^T A_{jm}^T = \\ &= \frac{n_i}{\gcd(n_i, n_j)} \sum_{m=1}^k \frac{n_m \gcd(n_i, n_j)}{\gcd(n_i, n_m) \gcd(n_m, n_j)} (A_{jm} B_{mi})^T = (HG)_{ij}^*. \end{aligned}$$

The rest is obvious.

- (ii) Let $H, G \in \mathcal{S}_{[n_1, \dots, n_k]}$. Then $H \equiv G$ implies $H^* \equiv G^*$. Thus the operation $*$ is well defined on $\mathcal{M}_{[n_1, \dots, n_k]}$.

Indeed, let $DH \equiv_\ell DG$. Then $DH^* \equiv_\ell H^T D \equiv_\ell G^T D \equiv_\ell DG^*$ and $H^* \equiv G^*$.

Now we are going to define $\text{Sp}_{[n_1, \dots, n_k]}$.

Definition 3.5. Denote $J = \text{diag}(J_2, \dots, J_2) \in \mathcal{M}_{[n_1, \dots, n_k]}$ where $J_2 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$

and put

$$\text{Sp}_{[n_1, \dots, n_k]} := \{H \in \mathcal{M}_{[n_1, \dots, n_k]} \mid H^* J H = J\}. \quad (3)$$

The following proposition implies that $\text{Sp}_{[n_1, \dots, n_k]}$ is a finite subgroup of the monoid $\mathcal{M}_{[n_1, \dots, n_k]}$.

Proposition 3.6. Let \mathcal{M} be a finite monoid and $x \mapsto x^*$ an involutive anti-homomorphism of \mathcal{M} (i.e. $(x^*)^* = x$ and $(xy)^* = y^*x^*$ for every $x, y \in \mathcal{M}$). Let $j \in \mathcal{M}$ be such that $j^*j = 1$. Then $\mathcal{G} = \{x \in \mathcal{M} \mid x^*jx = j\}$ is a group. Moreover, $\mathcal{G} = \{x \in \mathcal{M} \mid xjx^* = j\}$.

Proof. Let $x, y \in \mathcal{G}$. Then $(xy)^*j(xy) = y^*(x^*jx)y = y^*jy = j$. Hence $xy \in \mathcal{G}$ and \mathcal{G} is closed under multiplication. Further, since j has a left inverse, it is invertible, $jj^* = 1$ and thus $1, j, j^* \in \mathcal{G}$. For $x \in \mathcal{G}$ we have $x^*jx = j$, hence $(j^*x^*j)x = 1$. Thus x is invertible, $x^{-1} = j^*x^*j$ and $1 = xx^{-1} = xj^*x^*j$. It follows $j^* = xj^*x^*$ and applying the $*$ operation we get $j = xjx^* = (x^*)^*jx^*$, since $(x^*)^* = x$. Finally $x^* \in \mathcal{G}$, $x^{-1} = j^*x^*j \in \mathcal{G}$ and \mathcal{G} is a group. By a similar argument, $xjx^* = j$ implies $x^*jx = j$. \square

Corollary 3.7. $\text{Sp}_{[n_1, \dots, n_k]}$ is a finite subgroup of the monoid $\mathcal{M}_{[n_1, \dots, n_k]}$.

Proposition 3.8. Let $H = (h_{ij})_{i,j=1, \dots, 2k} \in \mathcal{M}_{[n_1, \dots, n_k]}$, $h_{ij} = \frac{n_{\lceil i/2 \rceil}}{\gcd(n_{\lceil i/2 \rceil}, n_{\lceil j/2 \rceil})} a_{ij}$ and $a_{ij} \in \mathbb{Z}_{n_{\lceil i/2 \rceil}}$ for $i, j = 1, \dots, 2k$. Then $H \in \text{Sp}_{[n_1, \dots, n_k]}$ if and only if

$$\sum_{m=1}^k \frac{n_{\lceil i/2 \rceil}}{\gcd(n_m, n_{\lceil i/2 \rceil})} \cdot \frac{n_m}{\gcd(n_m, n_{\lceil j/2 \rceil})} (a_{2m-1,i} a_{2m,j} - a_{2m-1,j} a_{2m,i}) \equiv_{n_{\lceil i/2 \rceil}} w_{ij}$$

for every $i, j = 1, \dots, 2k$ (where $J = (w_{ij})_{i,j=1, \dots, 2k} \in \text{Sp}_{[n_1, \dots, n_k]}$).

Proof. We only transcribe the equation $H^* J H = J$ using $h_{ij}^* = \frac{n_{\lceil i/2 \rceil}}{\gcd(n_{\lceil i/2 \rceil}, n_{\lceil j/2 \rceil})} a_{ji}$, $w_{2m-1,2m} = 1$, $w_{2m,2m-1} = -1$ for $m = 1, \dots, k$ and $w_{ij} = 0$ otherwise. \square

Due to 3.5 the new groups $\text{Sp}_{[n_1, \dots, n_k]}$ represent very specific generalization of symplectic groups over modular rings, thus providing sufficient reason for our notation. Clearly, for composite systems consisting of subsystems of equal dimensions $n_1 = \dots = n_k$, the new groups reduce to the well known symplectic groups [5]:

Corollary 3.9. *If $n_1 = \dots = n_k = n$, i.e. $N = n^k$, the symmetry group is $\mathrm{Sp}_{[n, \dots, n]} \cong \mathrm{Sp}_{2k}(\mathbb{Z}_n)$.*

These cases are of particular interest, since they uncover symplectic symmetry of k -partite systems composed of subsystems with the same dimensions. This circumstance was found, to our knowledge, first in [14] for $k = 2$ under additional assumption that $n = p$ is prime, leading to $\mathrm{Sp}_4(\mathbb{F}_p)$ over the field \mathbb{F}_p . We have generalized this result in [3] to bipartite systems with arbitrary (non-prime) $n = m$ yielding the symmetry group $\mathrm{Sp}_4(\mathbb{Z}_n)$ over the modular ring \mathbb{Z}_n . The above corollary 3.9 extends this fact also to multipartite systems. Similar result has independently been obtained in [15], where symmetries of tensored Pauli gradings of $\mathfrak{sl}_{n^k}(\mathbb{C})$ were investigated.

4. Characterization of $\mathrm{Sp}_{[n_1, \dots, n_k]}$

In this section we are going to prove theorem 4.7 describing by which elements the group $\mathrm{Sp}_{[n_1, \dots, n_k]}$ is generated. Let $n_1, \dots, n_k \in \mathbb{N}$ be again fixed numbers.

Definition 4.1. Let $\ell \in \mathbb{Z}$, $1 \leq i < j \leq k$. We define special matrices $G_{ij}(\ell) \in \mathcal{M}_{[n_1, \dots, n_k]}$ with 2×2 blocks

$$\left(G_{ij}(\ell) \right)_{rs} := \begin{cases} I_2 & \text{if } r = s \\ \frac{n_r}{\gcd(n_r, n_s)} \ell \cdot \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} & \text{if } (r, s) = (i, j), (j, i) \\ 0 & \text{otherwise} \end{cases}$$

where $r, s = 1, \dots, k$.

Further we note that

$$\begin{aligned} & \mathrm{SL}_2(\mathbb{Z}_{n_1}) \times \dots \times \mathrm{SL}_2(\mathbb{Z}_{n_k}) \cong \\ & \cong \left\{ \mathrm{diag}(H_1, \dots, H_k) \in \mathcal{M}_{[n_1, \dots, n_k]} \mid H_i \in \mathrm{M}_2(\mathbb{Z}_{n_i}) \text{ \& } \det H_i \equiv_{n_i} 1 \right\}. \end{aligned}$$

Thus we can assume $\mathrm{SL}_2(\mathbb{Z}_{n_1}) \times \dots \times \mathrm{SL}_2(\mathbb{Z}_{n_k})$ to be naturally embedded into $\mathrm{Sp}_{[n_1, \dots, n_k]}$.

Lemma 4.2. $G_{ij}(\ell) = G_{ij}(1)^\ell$ for every $\ell \in \mathbb{Z}$ and $1 \leq i < j \leq k$ and $G_{ij}(1) \in \mathrm{Sp}_{[n_1, \dots, n_k]}$.

Proof. First consider a permutation π of the set $\{1, \dots, k\}$. It induces an isomorphism $\varphi_\pi : \mathcal{M}_{[n_1, \dots, n_k]} \rightarrow \mathcal{M}_{[n_{\pi(1)}, \dots, n_{\pi(k)}]}$. It is clear that $H \in \mathrm{Sp}_{[n_1, \dots, n_k]}$ if and only if $\varphi_\pi(H) \in \mathrm{Sp}_{[n_{\pi(1)}, \dots, n_{\pi(k)}]}$ for every $H \in \mathcal{M}_{[n_1, \dots, n_k]}$. Hence it is enough to show our assertion for $G_{12}(\ell)$ only and this is equivalent to the case $k = 2$ which was already treated in [3, A.4], where $G_{12}(\ell)$ was denoted $r(\ell)$. \square

Remark 4.3. Let $u = (a, b)^T \in \mathbb{Z}^2$. Then there are $A, A' \in \mathrm{SL}_2(\mathbb{Z})$ such that $Au = (0, \gcd(a, b))^T$ and $A'u = (\gcd(a, b), 0)^T$. We can assume $u \neq 0$. Then there are $k, l \in \mathbb{Z}$ such that $ka + lb = \gcd(a, b) =: d$. Now just put $A = \begin{pmatrix} b/d & -a/d \\ k & l \end{pmatrix}$ and $A' = J_2 A$.

Now let \mathcal{G} denote the subgroup of $\mathrm{Sp}_{[n_1, \dots, n_k]}$ which is generated by $\mathrm{SL}_2(\mathbb{Z}_{n_1}) \times \dots \times \mathrm{SL}_2(\mathbb{Z}_{n_k})$ and $\{G_{ij}(1) \mid 1 \leq i < j \leq k\}$. We are going to prove theorem 4.7 that $\mathcal{G} = \mathrm{Sp}_{[n_1, \dots, n_k]}$. For this some auxiliary notions are needed.

Remark 4.4. (i) Consider the elements of $\mathcal{S}_{[n_1, \dots, n_k]}$ as $k \times k$ matrices of 2×2 blocks.

Let Σ_k be the set of all last (i.e. the k -th) columns of the elements of $\mathcal{S}_{[n_1, \dots, n_k]}$ and, similarly, let Σ_k^* be the set of all last (i.e. the k -th) rows of the elements of $\mathcal{S}_{[n_1, \dots, n_k]}$. Clearly, the involution $*$ on $\mathcal{S}_{[n_1, \dots, n_k]}$ induces a bijection $\Sigma_k \rightarrow \Sigma_k^*$ (we will use the same notation for it).

- (ii) The congruence \equiv on $\mathcal{S}_{[n_1, \dots, n_k]}$ induces naturally equivalences on Σ_k and Σ_k^* (we will use again the same notation for them and denote $[U]$ the equivalence class containing an element U). Hence it easily follows that $U, U' \in \Sigma_k$, $U \equiv U'$ and $H, H' \in \mathcal{S}_{[n_1, \dots, n_k]}$, $H \equiv H'$ imply $U^* \equiv (U')^*$ and $HU \equiv H'U'$. Moreover, $(HU)^* = U^*H^*$.
- (iii) Now, put $\Omega_k := \Sigma_k / \equiv$ and $\Omega_k^* := \Sigma_k^* / \equiv$. By (i), (ii) and 3.4, we have a well defined map $\Omega_k \rightarrow \Omega_k^*$ induced by $*$ and there is a natural action (via the matrix multiplication) of the ring $\mathcal{M}_{[n_1, \dots, n_k]}$ on the set Ω_k .
- (iv) Let $U, U' \in \Sigma_k$, $U \equiv U'$ and $T, T' \in \Sigma_k^*$, $T \equiv T'$. Then $TU \equiv_{n_k} T'U'$. (Clearly, there are $H, H' \in \mathcal{S}_{[n_1, \dots, n_k]}$ such that U (U') is the last column of H (H') and $H \equiv H'$. Similarly, there are $G, G' \in \mathcal{S}_{[n_1, \dots, n_k]}$ such that T (T') is the last row of G (G') and $G \equiv G'$. Then TU ($T'U'$) is the block on the (k, k) -position of the matrix GH ($G'H'$). By 3.2 part (vii) we have $GH \equiv G'H'$ and thus $TU \equiv_{n_k} T'U'$.)

Now we define the set

$$\Delta_k := \{[U] \in \Omega_k \mid U^*JU \equiv_{n_k} J_2\}. \quad (4)$$

It is by 4.4 part (iv) well defined. Using parts (ii) and (iii) we see that Δ_k is invariant under the action of the group $\text{Sp}_{[n_1, \dots, n_k]}$ (this action is a restriction of the action of $\mathcal{M}_{[n_1, \dots, n_k]}$ on Ω_k that was considered above).

Proposition 4.5. \mathcal{G} acts transitively on Δ_k .

Proof. In this proof we will consider an element from Ω_k as an ordered pair of its columns, i.e. as (v, u) where $v, u \in \mathcal{K} = \mathbb{Z}_{n_1}^2 \times \dots \times \mathbb{Z}_{n_k}^2$ are $2k$ -tuples. Note that for $v^0 = (0, \dots, 0, 1, 0)^T$ and $u^0 = (0, \dots, 0, 1)^T$ the pair (v^0, u^0) belongs to Δ_k .

Now assume that some $(v, u) \in \Delta_k$ is given. To prove our assertion, we construct for some $n \in \mathbb{N}$ a sequence of pairs ending with (v^0, u^0) , i.e. $(v, u) = (v_0, u_0), \dots, (v_n, u_n) = (v^0, u^0)$ in Δ_k and another sequence of matrices H_1, \dots, H_n in \mathcal{G} such that $(v_{j+1}, u_{j+1}) = H_{j+1}(v_j, u_j)$ for $j = 0, \dots, n-1$. We divide the proof into several steps. We put $d_{(i,j)} = \frac{n_i}{\gcd(n_i, n_j)}$ and note that $d_{(i,i)} = 1$.

(1) By 4.3, there are $B_i \in \text{SL}_2(\mathbb{Z}_{n_i})$ for $i = 1, \dots, k$ such that for $H_1 := \text{diag}(B_1, \dots, B_k) \in \mathcal{G}$ we have

$$u_1 := H_1 u = (d_{(1,k)}a_1, 0, \dots, d_{(k,k)}a_k, 0)^T$$

for some $a_i \in \mathbb{Z}_{n_i}$.

(2) Let

$$v_1 := (d_{(1,k)}b_1, d_{(1,k)}c_1, \dots, d_{(k,k)}b_k, d_{(k,k)}c_k)^T.$$

Then, by the definition of Δ_k , we have $\sum_{m=1}^k d_{(k,m)}d_{(m,k)}a_m c_m \equiv_{n_k} -1$. Put $H_2 := \text{diag}(I_2, \dots, I_2, B) \in \mathcal{G}$, where $B := \begin{pmatrix} 1 & 0 \\ c_k & 1 \end{pmatrix}$. Then

$$u_2 := H_2 u_1 = (d_{(1,k)}a_1, 0, \dots, d_{(k-1,k-1)}a_{k-1}, 0, a_k, a_k c_k)^T.$$

Next by induction on $1 \leq m \leq k-1$ we get that for $H_{m+2} := G_{mk}(c_m)$ (where $G_{ij}(\ell)$ was defined in 4.1)

$$\begin{aligned} u_{m+2} &:= H_{m+2}u_{m+1} = \\ &= (\dots, d_{(m+1,k)}a_{m+1}, 0, \dots, d_{(k-1,k)}a_{k-1}, 0, a_k, \left(a_k c_k + \sum_{i=1}^m d_{(k,i)}d_{(i,k)}a_i c_i\right))^T. \end{aligned}$$

Thus

$$u_{k+1} = (\dots, a_k, -1)^T.$$

(3) Using a similar argument as in step (1), we get that there is $H_{k+2} \in \mathcal{G}$ such that

$$u_{k+2} := H_{k+2}u_{k+1} = (0, d_{(1,k)}a'_1, \dots, 0, d_{(k-1,k-1)}a'_{k-1}, 1, 0)^T$$

for some $a'_i \in \mathbb{Z}_{n_i}$. Further put $H_{k+3} := G_{1,k}(-a'_1) \cdots G_{k,k}(-a'_k) \in \mathcal{G}$. Then, clearly,

$$u_{k+3} := H_{k+3}u_{k+2} = (0, \dots, 0, 1, 0)^T.$$

(4) Using again a similar argument as in step (1), we get that there is $H_{k+4} \in \mathcal{G}$ such that

$$u_{k+4} := H_{k+4}u_{k+3} = (0, \dots, 0, 1)^T$$

and

$$v_{k+4} := (0, d_{(1,k)}b'_1, \dots, 0, d_{(k-1,k)}b'_{k-1}, b', c')^T$$

for some $b'_i \in \mathbb{Z}_{n_i}$, $b', c' \in \mathbb{Z}_{n_k}$. Now we get from the defining equation (4) for Δ_k that $b' \equiv_{n_k} 1$. Put $B' := \begin{pmatrix} 1 & 0 \\ -c' & 1 \end{pmatrix}$. Then for $H_{k+5} := \text{diag}(I_2, \dots, I_2, B') \in \mathcal{G}$ we get that

$$u_{k+5} := H_{k+5}u_{k+4} = (0, \dots, 0, 1)^T$$

and

$$v_{k+5} := H_{k+5}v_{k+4} = (0, d_{(1,k)}b'_1, \dots, 0, d_{(k-1,k)}b'_{k-1}, 1, 0)^T.$$

So we are in an analogous situation to step (3) and thus there is $H_{k+6} \in \mathcal{G}$ such that

$$u_{k+6} := H_{k+6}u_{k+5} = (0, \dots, 0, 1)^T$$

stays unchanged and $v_{k+6} := H_{k+6}v_{k+5} = (0, \dots, 0, 1, 0)^T$. \square

Lemma 4.6. *Let $H \in \mathcal{M}_{[n_1, \dots, n_{k-1}]}$ and assume that $T \in \Sigma_{k-1}^*$ is such that $\begin{pmatrix} H & 0 \\ T & I_2 \end{pmatrix} \in \text{Sp}_{[n_1, \dots, n_k]}$. Then $T = 0$ and $H \in \text{Sp}_{[n_1, \dots, n_{k-1}]}$.*

Proof. There is $U \in \Sigma_k$ such that $T = U^*$. We have

$$\begin{pmatrix} J & 0 \\ 0 & J_2 \end{pmatrix} = \begin{pmatrix} H^* & U \\ 0 & I_2 \end{pmatrix} \begin{pmatrix} J & 0 \\ 0 & J_2 \end{pmatrix} \begin{pmatrix} H & 0 \\ U^* & I_2 \end{pmatrix} = \begin{pmatrix} H^* J H + U J_2 U^* & U J_2 \\ J_2 U^* & J_2 \end{pmatrix}.$$

Hence $U^* = 0$ and $H^* J H = J$. \square

Theorem 4.7. *The group $\text{Sp}_{[n_1, \dots, n_k]}$ is generated by $\text{SL}_2(\mathbb{Z}_{n_1}) \times \cdots \times \text{SL}_2(\mathbb{Z}_{n_k})$ and $\{G_{ij}(1) \mid 1 \leq i < j \leq k\}$.*

Proof. Let $G \in \text{Sp}_{[n_1, \dots, n_k]}$ and $U \in \Sigma_k$ be the last column of G . Then $U \in \Delta_k$ by 3.8. Hence by 4.5 there is $G' \in \mathcal{G}$ such that $G'G = \begin{pmatrix} H & 0 \\ T & I_2 \end{pmatrix}$ for some $H \in \mathcal{M}_{[n_1, \dots, n_{k-1}]}$ and $T \in \Sigma_{k-1}^*$. Using 4.6, we have $G'G = \begin{pmatrix} H & 0 \\ 0 & I_2 \end{pmatrix}$ with $H \in \text{Sp}_{[n_1, \dots, n_{k-1}]}$. Now, by repeating this argument several times, we find $\tilde{G} \in \mathcal{G}$ such that $\tilde{G}G = I_{2k}$. Hence $G = \tilde{G}^{-1} \in \mathcal{G}$ and we conclude with $\text{Sp}_{[n_1, \dots, n_k]} = \mathcal{G}$. \square

5. The normalizer of $\mathcal{P}_{(n_1, \dots, n_k)}$

In this section the normalizer is completely described and the main theorem 5.9 is proved. It contains our principal result that the symmetry group, being the quotient of the normalizer, is indeed isomorphic to $\text{Sp}_{[n_1, \dots, n_k]}$.

For proving the isomorphism between the group $\mathcal{N}(\mathcal{P}_{(n_1, \dots, n_k)})/\mathcal{P}_{(n_1, \dots, n_k)}$ and $\text{Sp}_{[n_1, \dots, n_k]}$, we will consider elements of $\mathcal{M}_{[n_1, \dots, n_k]}$ as matrices $2k \times 2k$ instead of taking them as matrices $k \times k$ of blocks 2×2 , as we did so far. More precisely, $H \in \text{Sp}_{[n_1, \dots, n_k]}$ will be treated as $H = (h_{ij})_{i,j=1, \dots, 2k}$, where

$$h_{ij} = \frac{n_{\lceil i/2 \rceil}}{\gcd(n_{\lceil i/2 \rceil}, n_{\lceil j/2 \rceil})} a_{ij}$$

for some $a_{ij} \in \mathbb{Z}_{n_{\lceil i/2 \rceil}}$ and all $i, j = 1, \dots, 2k$.

Definition 5.1. Define

$$\mathcal{N}(\mathcal{P}_{(n_1, \dots, n_k)}) := N_{\text{Int}(\text{GL}_{n_1 \dots n_k}(\mathbb{C}))}(\mathcal{P}_{(n_1, \dots, n_k)}),$$

the normalizer of $\mathcal{P}_{(n_1, \dots, n_k)}$ in $\text{Int}(\text{GL}_{n_1 \dots n_k}(\mathbb{C}))$. Further define

$$\mathcal{N}(\mathcal{P}_n) := N_{\text{Int}(\text{GL}_n(\mathbb{C}))}(\mathcal{P}_n),$$

the normalizer of \mathcal{P}_n in $\text{Int}(\text{GL}_n(\mathbb{C}))$, and

$$\mathcal{N}(\mathcal{P}_{n_1}) \times \dots \times \mathcal{N}(\mathcal{P}_{n_k}) := \{\text{Ad}_{M_1 \otimes \dots \otimes M_k} \mid M_i \in \mathcal{N}(\mathcal{P}_{n_i})\} \subseteq \text{Int}(\text{GL}_{n_1 \dots n_k}(\mathbb{C})).$$

Remark 5.2.

- (i) Clearly, $\mathcal{N}(\mathcal{P}_{n_1}) \times \dots \times \mathcal{N}(\mathcal{P}_{n_k}) \subseteq \mathcal{N}(\mathcal{P}_{(n_1, \dots, n_k)})$.
- (ii) Consider now the usual natural homomorphism

$$\Psi : \mathcal{N}(\mathcal{P}_{(n_1, \dots, n_k)}) \rightarrow \text{Aut}(\mathcal{P}_{(n_1, \dots, n_k)})$$

given by

$$\Psi(\text{Ad}_M)(\text{Ad}_X) := \text{Ad}_M \text{Ad}_X \text{Ad}_M^{-1}$$

for every $\text{Ad}_M \in \mathcal{N}(\mathcal{P}_{(n_1, \dots, n_k)})$ and $\text{Ad}_X \in \mathcal{P}_{(n_1, \dots, n_k)}$.

We have $\ker(\Psi) = C_{\text{Int}(\text{GL}_{n_1 \dots n_k}(\mathbb{C}))}(\mathcal{P}_{(n_1, \dots, n_k)}) = \mathcal{P}_{(n_1, \dots, n_k)}$, by lemma 2.3.

- (iii) Further we put

$$\lambda_{ij} = \exp\left(2\pi i \frac{w_{ij}}{n_{\lceil i/2 \rceil}}\right)$$

for $i, j = 1, \dots, 2k$, where w_{ij} are the entries of the matrix $J \in \text{Sp}_{[n_1, \dots, n_k]}$ defined in 3.5. Using (2) and (1) we can write the commutation relations

$$A_i^m A_j^n = \lambda_{ij}^{mn} A_j^n A_i^m \tag{5}$$

for all pairs $i, j = 1, \dots, 2k$ and $m, n \in \mathbb{Z}$.

Lemma 5.3. $\Phi\Psi(\mathcal{N}(\mathcal{P}_{(n_1, \dots, n_k)})) \subseteq \text{Sp}_{[n_1, \dots, n_k]}$.

Proof. Let $\text{Ad}_G \in \mathcal{N}(\mathcal{P}_{(n_1, \dots, n_k)})$, where $G \in \text{GL}_{n_1 \dots n_k}(\mathbb{C})$. By 3.3, there is $H = (h_{ij})_{i,j=1, \dots, 2k} \in \mathcal{M}_{[n_1, \dots, n_k]}$ such that $\Phi\Psi(\text{Ad}_G) = H$. Especially for $e_j = \text{Ad}_{A_j}$ we have

$$\text{Ad}_{GA_jG^{-1}} = \Psi(\text{Ad}_G)(e_j) = \prod_{i=1}^{2k} e_i^{h_{ij}} = \prod_{i=1}^{2k} \text{Ad}_{A_i^{h_{ij}}}.$$

So there are constants $0 \neq \nu_j \in \mathbb{C}$ such that

$$GA_jG^{-1} = \nu_j A_1^{h_{1,j}} \dots A_{2k}^{h_{2k,j}}$$

for $j = 1, \dots, 2k$. Further,

$$\begin{aligned} GA_iA_jG^{-1} &= GA_iG^{-1}GA_jG^{-1} = \nu_i\nu_j A_1^{h_{1,i}} \dots A_{2k}^{h_{2k,i}} A_1^{h_{1,j}} \dots A_{2k}^{h_{2k,j}} = \\ &= \nu_i\nu_j \left(\prod_{m=1}^k \lambda_{2m,2m-1}^{h_{2m,i}h_{2m-1,j}} \right) A_1^{h_{1,i}+h_{1,j}} \dots A_{2k}^{h_{2k,i}+h_{2k,j}} \end{aligned}$$

using the commutation relations (5) (where the only non-commuting elements are pairs A_{2m-1}, A_{2m} for $m = 1, \dots, k$). On the other hand,

$$GA_iA_jG^{-1} = \lambda_{ij}GA_jA_iG^{-1} = \nu_i\nu_j\lambda_{ij} \left(\prod_{m=1}^k \lambda_{2m,2m-1}^{h_{2m,j}h_{2m-1,i}} \right) A_1^{h_{1,i}+h_{1,j}} \dots A_{2k}^{h_{2k,i}+h_{2k,j}}.$$

Thus

$$\prod_{m=1}^k e^{-2\pi i(h_{2m,i}h_{2m-1,j}/n_m)} = \lambda_{ij} \prod_{m=1}^k e^{-2\pi i(h_{2m,j}h_{2m-1,i}/n_m)}$$

for every $i, j = 1, \dots, 2k$, i.e.

$$\exp\left(2\pi i\left(-\frac{w_{ij}}{n_{\lceil i/2 \rceil}} + \sum_{m=1}^k \frac{h_{2m-1,i}h_{2m,j} - h_{2m-1,j}h_{2m,i}}{n_m}\right)\right) = 1.$$

Since $h_{ij} = \frac{n_{\lceil i/2 \rceil}}{\gcd(n_{\lceil i/2 \rceil}, n_{\lceil j/2 \rceil})} a_{ij}$ for some $a_{ij} \in \mathbb{Z}_{n_{\lceil i/2 \rceil}}$, by 3.3 we get

$$-\frac{w_{ij}}{n_{\lceil i/2 \rceil}} + \sum_{m=1}^k \frac{n_m}{\gcd(n_m, n_{\lceil i/2 \rceil}) \gcd(n_m, n_{\lceil j/2 \rceil})} (a_{2m-1,i}a_{2m,j} - a_{2m-1,j}a_{2m,i}) \in \mathbb{Z}.$$

This means that

$$\sum_{m=1}^k \frac{n_{\lceil i/2 \rceil}}{\gcd(n_m, n_{\lceil i/2 \rceil})} \cdot \frac{n_m}{\gcd(n_m, n_{\lceil j/2 \rceil})} (a_{2m-1,i}a_{2m,j} - a_{2m-1,j}a_{2m,i}) \equiv_{n_{\lceil i/2 \rceil}} w_{ij}$$

for every $i, j = 1, \dots, 2k$. Hence, by 3.8, $H \in \text{Sp}_{[n_1, \dots, n_k]}$. \square

Definition 5.4. Let $1 \leq i < j \leq k$. Put

$$T_{ij} = I_{n_{i+1} \dots n_{j-1}} \otimes Q_{n_j}^{\frac{n_j}{\gcd(n_i, n_j)}}$$

and

$$R_{ij} = I_{n_1 \dots n_{i-1}} \otimes \text{diag}(I_{n_{i+1} \dots n_j}, T_{ij}, \dots, T_{ij}^{n_i-1}) \otimes I_{n_{j+1} \dots n_k}.$$

Remark 5.5. For a ring \mathcal{R} , $M_n(\mathcal{R})$ is the ring of $n \times n$ matrices with entries from \mathcal{R} . For $a \in \mathcal{R}$ denote $Q_{[a]} := \text{diag}(1, a, a^2, \dots, a^{n-1}) \in M_n(\mathcal{R})$ and $P \in M_n(\mathcal{R})$, where $(P)_{i,j} := \delta_{i,j-1} \cdot 1_{\mathcal{R}}$ for $i, j \in \mathbb{Z}_n$. Let E denote the identity matrix.

- (i) Let $a \in \mathcal{R}$ be such that $a^n = 1$. Then $PQ_{[a]} = (aE)Q_{[a]}P$.
- (ii) Let $a, b, \omega \in \mathcal{R}$ be such that $ab = \omega ba$. Then $Q_{[a]}(bE) = Q_{[\omega]}(bE)Q_{[a]}$.

Lemma 5.6. *Let $1 \leq i < j \leq k$. Then $\text{Ad}_{R_{ij}} \in \mathcal{N}(\mathcal{P}_{(n_1, \dots, n_k)})$ and $\Phi\Psi(\text{Ad}_{R_{ij}}) = G_{ij}(-1) \in \text{Sp}_{[n_1, \dots, n_k]}$.*

Proof. R_{ij} is a regular diagonal matrix, so are A_{2m} , $m = 1, \dots, k$, and thus these matrices commute. Further, for m such that $1 \leq m < i$ or $j < m \leq k$, the matrices R_{ij} and A_{2m-1} also commute. Let now m be such that $i < m < j$, then

$$A_{2m-1} = I_{n_1 \dots n_{i-1}} \otimes \text{diag}(U, U, \dots, U) \otimes I_{n_{j+1} \dots n_k},$$

where $U = I_{n_{i+1} \dots n_{m-1}} \otimes P_{n_m} \otimes I_{n_{m+1} \dots n_{j-1}} \otimes I_{n_j}$ and

$$R_{ij} = I_{n_1 \dots n_{i-1}} \otimes \text{diag}(V^0, V^1, \dots, V^{n_i-1}) \otimes I_{n_{j+1} \dots n_k},$$

where $V = I_{n_{i+1} \dots n_{m-1}} \otimes I_{n_m} \otimes I_{n_{m+1} \dots n_{j-1}} \otimes Q_{n_j}^{\frac{n_j}{\gcd(n_i, n_j)}}$. Hence $UV = VU$ and we have the commutativity of R_{ij} and A_{2m-1} again.

Now we use 4.5 to treat the remaining cases. Put $n = n_i$, $\mathcal{R} = M_{n_{i+1} \dots n_j}(\mathbb{C})$ and $a = T_{ij}$. By 5.5(1), we have

$$\begin{aligned} & \text{diag}(T_{ij}^0, T_{ij}, T_{ij}^2, \dots, T_{ij}^{n_i-1})(P_{n_i} \otimes I_{n_{i+1} \dots n_j}) \left(\text{diag}(T_{ij}^0, T_{ij}, T_{ij}^2, \dots, T_{ij}^{n_i-1}) \right)^{-1} = \\ & = Q_{[a]} P Q_{[a]}^{-1} = P(aE)^{-1} = (P_{n_i} \otimes I_{n_{i+1} \dots n_j})(I_{n_i} \otimes T_{ij})^{-1}. \end{aligned}$$

Tensoring this with $I_{n_1 \dots n_{i-1}}$ from the left and with $I_{n_{j+1} \dots n_k}$ from the right we get

$$R_{ij} A_{2i-1} R_{ij}^{-1} = A_{2i-1} A_{2j}^{-\frac{n_j}{\gcd(n_i, n_j)}}.$$

Put $b = I_{n_{i+1} \dots n_{j-1}} \otimes P_{n_j}$ and $\omega = e^{-2\pi i / \gcd(n_i, n_j)} \cdot I_{n_{i+1} \dots n_j}$. Then $ab = \omega ba$ and by 5.5(2) we have

$$\begin{aligned} & \text{diag}(T_{ij}^0, T_{ij}, T_{ij}^2, \dots, T_{ij}^{n_i-1})(I_{n_i \dots n_{j-1}} \otimes P_{n_j}) \left(\text{diag}(T_{ij}^0, T_{ij}, T_{ij}^2, \dots, T_{ij}^{n_i-1}) \right)^{-1} = \\ & = Q_{[a]}(bE)Q_{[a]}^{-1} = Q_{[\omega]}(bE) = (Q_{n_i} \otimes I_{n_{i+1} \dots n_j})^{-\frac{n_i}{\gcd(n_i, n_j)}} (I_{n_i \dots n_{j-1}} \otimes P_{n_j}) \end{aligned}$$

Tensoring this with $I_{n_1 \dots n_{i-1}}$ from the left and with $I_{n_{j+1} \dots n_k}$ from the right we get

$$R_{ij} A_{2j-1} R_{ij}^{-1} = A_{2i}^{-\frac{n_i}{\gcd(n_i, n_j)}} A_{2j-1}.$$

We conclude with $\Phi\Psi(\text{Ad}_{R_{ij}}) = G_{ij}(-1)$, where $G_{ij}(\ell)$ was defined in 4.1. \square

Remark 5.7. Now the results obtained in [13] have to be recalled since they will be used in this and in the next section. They correspond to the case $k = 1$ with $n = n_1$. Using our notation we get that $\Phi\Psi(\mathcal{N}(\mathcal{P}_n)) = \text{SL}_2(\mathbb{Z}_n)$. Further, the group $\text{SL}_2(\mathbb{Z}_n)$ is generated by $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ and the group $\mathcal{N}(\mathcal{P}_n)$ is generated by $\text{Ad}_{P_n}, \text{Ad}_{Q_n}, \text{Ad}_{D_n}$ and Ad_{S_n} , where

$$(D_n)_{ij} := \delta_{ij} \varepsilon^{-i} \omega_n^{\binom{i}{2}}$$

with $\varepsilon = \sqrt{-1}$ for n even and $\varepsilon = 1$ for n odd, and

$$(S_n)_{ij} := \omega_n^{ij} / \sqrt{n}.$$

It was shown in [13] that $\Phi\Psi(D_n) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, $\Phi\Psi(S_n) = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ and $\ker(\Phi\Psi) = \mathcal{P}_n$.

As an immediate consequence we have the following proposition.

Proposition 5.8. $\Phi\Psi(\mathcal{N}(\mathcal{P}_{n_1}) \times \cdots \times \mathcal{N}(\mathcal{P}_{n_k})) = \text{SL}_2(\mathbb{Z}_{n_1}) \times \cdots \times \text{SL}_2(\mathbb{Z}_{n_k})$.

Finally we arrive at the announced main theorems.

Theorem 5.9. (i) $\mathcal{N}(\mathcal{P}_{(n_1, \dots, n_k)})/\mathcal{P}_{(n_1, \dots, n_k)} \cong \text{Sp}_{[n_1, \dots, n_k]}$

(ii) The group $\mathcal{N}(\mathcal{P}_{(n_1, \dots, n_k)})$ is generated by $\mathcal{N}(\mathcal{P}_{n_1}) \times \cdots \times \mathcal{N}(\mathcal{P}_{n_k})$ and $\{\text{Ad}_{R_{ij}} \mid 1 \leq i < j \leq k\}$.

Proof. (i) By 4.7, $\text{Sp}_{[n_1, \dots, n_k]}$ is generated by $\{G_{ij}(1) \mid 1 \leq i < j \leq k\}$ and $\text{SL}_2(\mathbb{Z}_{n_1}) \times \cdots \times \text{SL}_2(\mathbb{Z}_{n_k})$. Hence, by 5.3, 5.6 and 5.8, $\Phi\Psi(\mathcal{N}(\mathcal{P}_{(n_1, \dots, n_k)})) = \text{Sp}_{[n_1, \dots, n_k]}$. Using 3.3 and $\ker(\Psi) = \mathcal{P}_{(n_1, \dots, n_k)}$ we get $\ker(\Phi\Psi) = \mathcal{P}_{(n_1, \dots, n_k)}$.

(ii) Let \mathcal{N} be a subgroup of $\mathcal{N}(\mathcal{P}_{(n_1, \dots, n_k)})$ generated by $\mathcal{N}(\mathcal{P}_{n_1}) \times \cdots \times \mathcal{N}(\mathcal{P}_{n_k})$ and $\{\text{Ad}_{R_{ij}} \mid 1 \leq i < j \leq k\}$. Then $\ker(\Phi\Psi) = \mathcal{P}_{(n_1, \dots, n_k)} \subseteq \mathcal{N}(\mathcal{P}_{n_1}) \times \cdots \times \mathcal{N}(\mathcal{P}_{n_k}) \subseteq \mathcal{N}$ and, by 5.6, 5.8 and 4.7, $\Phi\Psi(\mathcal{N}) = \text{Sp}_{[n_1, \dots, n_k]}$. Hence $\mathcal{N} = \mathcal{N}(\mathcal{P}_{(n_1, \dots, n_k)})$. \square

Theorem 5.10. There is a group $\mathcal{G}_{(n_1, \dots, n_k)} \subseteq \text{U}_{n_1 \cdots n_k}(\mathbb{C})$ such that $\mathcal{N}(\mathcal{P}_{(n_1, \dots, n_k)}) = \{\text{Ad}_M \mid M \in \mathcal{G}_{(n_1, \dots, n_k)}\}$. In particular, $\mathcal{G}_{(n_1, \dots, n_k)}$ is generated by the matrices

$$I_{n_1 \cdots n_{i-1}} \otimes P_{n_i} \otimes I_{n_{i+1} \cdots n_k}$$

$$I_{n_1 \cdots n_{i-1}} \otimes Q_{n_i} \otimes I_{n_{i+1} \cdots n_k}$$

$$I_{n_1 \cdots n_{i-1}} \otimes D_{n_i} \otimes I_{n_{i+1} \cdots n_k}$$

$$I_{n_1 \cdots n_{i-1}} \otimes S_{n_i} \otimes I_{n_{i+1} \cdots n_k}$$

for $i = 1, \dots, k$ and

$$R_{ij}$$

for $1 \leq i < j \leq k$.

Proof. Follows immediately from 5.7 and 5.9. \square

6. Mutually unbiased bases and the symmetry group

In this section we turn to the special cases described in corollary 3.9, with $n_1 = \cdots = n_k = p$, where p is a prime. For such multipartite systems composed of subsystems with the same prime dimension p the Hilbert space is $\ell^2(\mathbb{Z}_p) \otimes \cdots \otimes \ell^2(\mathbb{Z}_p) \cong \ell^2(\mathbb{Z}_{p^k})$ and the symmetry group is $\text{Sp}_{[p, \dots, p]} \cong \text{Sp}_{2k}(\mathbb{Z}_p)$. Our goal is to use the symmetry group for an alternative proof of existence of a maximal set of mutually unbiased bases (MUBs) \ddagger in the Hilbert space of prime power dimension.

It is known that the number of mutually unbiased bases in a Hilbert space of dimension N must not exceed $N+1$ [6]. It is also well known that the maximal number $N+1$ is attained for N being prime or power of a prime. However, the determination of the maximal number of mutually unbiased bases for other dimensions N remains an open problem as yet.

Note that in this section the letter k will be replaced by n , thus an n -partite system is considered and the respective Hilbert space $\ell^2(\mathbb{Z}_{p^n})$ is taken with the standard inner product.

Essentially an idea of Bandyopadhyay, Boykin, Roychowdhury and Vatan [7] is used, but we provide a different proof. First we recall their main point.

\ddagger In the Hilbert space $\ell^2(\mathbb{Z}_N)$ let $\{e_i\}_{i=1}^N$, $\{f_j\}_{j=1}^N$ be two orthonormal bases. They are mutually unbiased, if $|\langle e_i, f_j \rangle| = 1/\sqrt{N}$ for all $i, j = 1, \dots, N$. In physical terms, if the system is in one of the states e_i , then the probabilities to find the system in any of the states f_j are all equal to $1/N$.

Denote

$$\Pi_p(n) := \{M_1 \otimes \cdots \otimes M_n \in \text{GL}_{p^n}(\mathbb{C}) \mid M_i \in \Pi_p\}.$$

For $\alpha = (k_1, \dots, k_n, \ell_1, \dots, \ell_n)^T \in \mathbb{Z}_p^{2n}$ put

$$A[\alpha] := Q_p^{k_1} P_p^{\ell_1} \otimes \cdots \otimes Q_p^{k_n} P_p^{\ell_n} \in \Pi_p(n).$$

For a $2n \times n$ matrix U over \mathbb{Z}_p assign a set of operators

$$\mathcal{C}(U) := \{A[\alpha_i] \mid i = 1, \dots, n\},$$

where α_i is the i -th column of the matrix U .

MUBs are now constructed as orthonormal sets of common eigenvectors of mutually commuting operators from $\mathcal{C}(U)$ for suitably chosen U . Using the commutation relations for P and Q one easily gets that

$$A[\alpha] \text{ and } A[\beta] \text{ commute if and only if } \alpha^T J' \beta = 0, \text{ where } J' := \begin{pmatrix} 0 & -I_n \\ I_n & 0 \end{pmatrix}.$$

Thus $\mathcal{C}(U)$ consists of mutually commuting operators if and only if $U^T J' U = 0$.

Now a special system $(*)$ of such matrices fulfilling this condition is chosen, namely

$$\begin{pmatrix} I_n \\ 0 \end{pmatrix} \text{ and } \begin{pmatrix} A_i \\ I_n \end{pmatrix} \text{ for } i = 1, \dots, p^n, \quad (*)$$

where $A_i \in M_n(\mathbb{Z}_p)$ are symmetric and $A_i - A_j$ are regular for $i \neq j$. The existence of such a system is shown further, see 6.8. In the following, $\mathcal{C}(U)$ will always denote such a set of mutually commuting operators.

We will now apply our previous results concerning the symmetry group to get a different proof that the system $(*)$ indeed provides a set of $p^n + 1$ mutually unbiased bases. Moreover, we will show that there is a group generating the MUBs from the canonical basis via a natural action.

As already mentioned, we consider the case $n_i = p$ for each $i = 1, \dots, n$. Then the phase space $\mathcal{P}_{(p, \dots, p)} \cong (\mathbb{Z}_p)^{2n}$ is a vector space of dimension $2n$ over \mathbb{Z}_p . In proposition 3.3 we have considered the homomorphism

$$\mathcal{N}(\mathcal{P}_{(p, \dots, p)}) \xrightarrow{\Phi} \text{End}(\mathcal{P}_{(p, \dots, p)}) \cong \text{End}(\mathbb{Z}_p^2 \times \cdots \times \mathbb{Z}_p^2) \cong \mathcal{M}_{[p, \dots, p]}$$

where the isomorphism $\text{End}(\mathcal{P}_{(p, \dots, p)}) \cong \mathcal{M}_{[p, \dots, p]}$ was given with respect to the basis $(\text{Ad}_{A_1}, \dots, \text{Ad}_{A_{2n}})$ of $\mathcal{P}_{(p, \dots, p)}$, where $A_{2i-1} = I_{p^{i-1}} \otimes P_p \otimes I_{p^{n-i}}$ and $A_{2i} = I_{p^{i-1}} \otimes Q_p \otimes I_{p^{n-i}}$ for $i = 1, \dots, n$.

Here it is useful to take a differently ordered basis, namely

$$(\text{Ad}_{A_2}, \text{Ad}_{A_4}, \dots, \text{Ad}_{A_{2n}}, \text{Ad}_{A_1}, \text{Ad}_{A_3}, \dots, \text{Ad}_{A_{2n-1}}).$$

Then the corresponding automorphism of $\mathcal{M}_{[p, \dots, p]} = M_{2n}(\mathbb{Z}_p)$, given by the above permutation matrix, transforms the symmetry group $\text{Sp}_{[p, \dots, p]}$ into the symplectic group over \mathbb{Z}_p [5]

$$\text{Sp}_{2n}(\mathbb{Z}_p) := \{H \in M_{2n}(\mathbb{Z}_p) \mid H^T J' H = J'\}.$$

Thus we can formulate our result as follows:

Proposition 6.1. *There is a surjective homomorphism*

$$\chi : \mathcal{N}(\mathcal{P}_{(p, \dots, p)}) \rightarrow \text{Sp}_{2n}(\mathbb{Z}_p)$$

such that

$$\text{Ad}_M \text{Ad}_{A[\alpha]} \text{Ad}_M^{-1} = \text{Ad}_{A[\chi(\text{Ad}_M)\alpha]}$$

for every $\alpha \in \mathbb{Z}_p^{2n}$ and $\text{Ad}_M \in \mathcal{N}(\mathcal{P}_{(p, \dots, p)})$, where $M \in \text{U}_{p^n}(\mathbb{C})$.

Remark 6.2. Let $\text{Ad}_M \in \mathcal{N}(\mathcal{P}_{(p,\dots,p)})$, $U \in \mathbb{Z}_p^{2n \times n}$ and α_i be the i -th column of U . Then the above property can be reformulated: for every $i = 1, \dots, n$ there is $0 \neq \lambda_i \in \mathbb{C}$ such that

$$M \cdot A[\alpha_i] \cdot M^{-1} = \lambda_i A[\chi(\text{Ad}_M)\alpha_i].$$

Moreover, if $u \in \ell_{p^n}$ is a common eigenvector of the set of operators $\mathcal{C}(U)$, then Mu is a common eigenvector of the set of operators $\mathcal{C}(\chi(\text{Ad}_M)U)$.

Proposition 6.3. Let $A, B \in M_n(\mathbb{Z}_p)$ be symmetric and $A - B$ be a regular matrix. Then:

- (i) There is $H \in \text{Sp}_{2n}(\mathbb{Z}_p)$ such that $H \begin{pmatrix} I_n \\ 0 \end{pmatrix} = \begin{pmatrix} I_n \\ 0 \end{pmatrix}$ and $H \begin{pmatrix} A \\ I_n \end{pmatrix} = \begin{pmatrix} 0 \\ I_n \end{pmatrix}$.
- (ii) There is $G \in \text{Sp}_{2n}(\mathbb{Z}_p)$ such that $G \begin{pmatrix} A \\ I_n \end{pmatrix} = \begin{pmatrix} I_n \\ 0 \end{pmatrix}$ and $G \begin{pmatrix} B \\ I_n \end{pmatrix} = \begin{pmatrix} 0 \\ D \end{pmatrix}$ for some regular $D \in M_n(\mathbb{Z}_p)$.

Proof. Note that for $A \in M_n(\mathbb{Z}_p)$, $\begin{pmatrix} I_n & A \\ 0 & I_n \end{pmatrix}$ belongs to $\text{Sp}_{2n}(\mathbb{Z}_p)$ if and only if A is symmetric. Put $H = \begin{pmatrix} I_n & -A \\ 0 & I_n \end{pmatrix}$ and $G = \begin{pmatrix} (A-B)^{-1} & -(A-B)^{-1}B \\ -I_n & A \end{pmatrix}$. \square

Remark 6.4. For $m \in \mathbb{N}$ the matrix $S_m \in M_m(\mathbb{C})$ introduced in 5.7 is unitary and induces the discrete Fourier transform

$$S_m Q_m S_m^{-1} = P_m \quad \text{and} \quad S_m P_m S_m^{-1} = Q_m^{-1}.$$

Thus for $\text{Ad}_{S_p \otimes \dots \otimes S_p} \in \mathcal{N}(\mathcal{P}_{(p,\dots,p)})$ we have

$$\chi(\text{Ad}_{S_p \otimes \dots \otimes S_p}) = J' \quad \text{and} \quad J' \begin{pmatrix} I_n \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ I_n \end{pmatrix}.$$

Corollary 6.5. Let $U = \begin{pmatrix} I_n \\ 0 \end{pmatrix}$ or $U = \begin{pmatrix} A \\ I_n \end{pmatrix}$ where $A \in M_n(\mathbb{Z}_p)$ is a symmetric matrix. Then there is an orthonormal basis of common eigenvectors for the mutually commuting operator set $\mathcal{C}(U)$.

Proof. For $U = \begin{pmatrix} I_n \\ 0 \end{pmatrix}$ clearly the standard basis \mathcal{E} is the desired basis. Let $U = \begin{pmatrix} A \\ I_n \end{pmatrix}$, where $A \in M_n(\mathbb{Z}_p)$ is a symmetric matrix. By 6.3 (putting e.g. $B = A - I_n$) there are $G \in \text{Sp}_{2n}(\mathbb{Z}_p)$ such that $\begin{pmatrix} A \\ I_n \end{pmatrix} = G^{-1} \begin{pmatrix} I_n \\ 0 \end{pmatrix}$ and $M \in \text{U}_{p^n}(\mathbb{C})$ such that $\text{Ad}_M \in \mathcal{N}(\mathcal{P}_{(p,\dots,p)})$ and $\chi(\text{Ad}_M) = G$. Using 6.2 and the unitarity of M , we obtain the desired basis as $\{M^{-1}e \mid e \in \mathcal{E}\}$. \square

Proposition 6.6. (i) Let $D \in M_n(\mathbb{Z}_p)$ be regular and \mathcal{B} be a basis of common eigenvectors for $\mathcal{C} \begin{pmatrix} 0 \\ D \end{pmatrix}$. Then \mathcal{B} is also a basis of common eigenvectors for $\mathcal{C} \begin{pmatrix} I_n \\ 0 \end{pmatrix}$.

(ii) Let \mathcal{B} be an orthonormal basis of common eigenvectors for $\mathcal{C} \begin{pmatrix} I_n \\ 0 \end{pmatrix}$ and u from \mathcal{B} . Then there is a complex unit λ such that λu belongs to the standard basis \mathcal{E} of \mathbb{C}^{p^n} .

(iii) Let \mathcal{B} (\mathcal{B}' , respectively) be an orthonormal basis of common eigenvectors for $\mathcal{C} \begin{pmatrix} I_n \\ 0 \end{pmatrix}$ ($\mathcal{C} \begin{pmatrix} 0 \\ D \end{pmatrix}$, respectively). Then \mathcal{B} and \mathcal{B}' are mutually unbiased.

Proof. (i) Since D is invertible, we have that for every $i = 1, \dots, n$, $I_{p^{i-1}} \otimes P_i \otimes I_{p^{n-i}}$ lies in the group generated by $\{A[\alpha_j] \mid j = 1, \dots, n\}$ where α_j is the j -th column of $\begin{pmatrix} 0 \\ D \end{pmatrix}$. Our assertion now follows immediately.

(ii) Let \mathcal{E}_p be the standard basis of \mathbb{C}^p . Since u is an eigenvector of $Q_p \otimes I_{p^{n-1}}$ it is of the form $u = e_{i_1} \otimes v$ for some $i_1 = 1, \dots, p$ and $v \in \mathbb{C}^{p^{n-1}}$. Now, $u = e_{i_1} \otimes v$ is an eigenvector of $I_p \otimes Q_p \otimes I_{p^{n-2}}$, hence it is of the form $u = e_{i_1} \otimes e_{i_2} \otimes w$ for some $i_2 = 1, \dots, p$ and $w \in \mathbb{C}^{p^{n-2}}$. Repeating this argument we get that $u = \lambda e_{i_1} \otimes \dots \otimes e_{i_n}$ for $i_j = 1, \dots, p$ and $\lambda \in \mathbb{C}$. Since u is normalized, it follows that $|\lambda| = 1$.

(iii) Put $M = S_p \otimes \cdots \otimes S_p \in \text{U}_{p^n}(\mathbb{C})$ (see 6.4). By 6.2 and 6.4, $M^{-1}\mathcal{B}'$ is an orthonormal basis of common eigenvectors for $\mathcal{C}\left(\begin{smallmatrix} I_n \\ 0 \end{smallmatrix}\right)$. Hence, by (ii), there are matrices $R_1, R_2 \in \text{GL}_{p^n}(\mathbb{C})$ with only one non-zero entry (a complex unit) in each column and row, such that $M^{-1}\mathcal{B}' = R_1\mathcal{E}$ and $\mathcal{B} = R_2\mathcal{E}$. Now, let u be from $\mathcal{B} = R_2\mathcal{E}$ and u' from $\mathcal{B}' = MR_1\mathcal{E}$. Then there are $i, j \in \{1, \dots, p^n\}$ such that $u = R_2e_i$ and MR_1e_j with e_i, e_j from \mathcal{E} . Hence

$$|(u, u')| = |(R_2e_i, MR_1e_j)| = |(R_2^T MR_1)_{ij}| = 1/\sqrt{p^n},$$

i.e. \mathcal{B} and \mathcal{B}' are mutually unbiased. \square

Corollary 6.7. *Let U and U' be distinct matrices from the system $(*)$, and \mathcal{B} and \mathcal{B}' be orthonormal bases of common eigenvectors for $\mathcal{C}(U)$ and $\mathcal{C}(U')$, respectively. Then \mathcal{B} and \mathcal{B}' are mutually unbiased.*

Proof. By 6.3, 6.4 and 5.10 there is $M \in \text{U}_{p^n}(\mathbb{C})$ such that $\chi(\text{Ad}_M)U = \begin{pmatrix} I_n \\ 0 \end{pmatrix}$ and $\chi(\text{Ad}_M)U' = \begin{pmatrix} 0 \\ D \end{pmatrix}$ for some regular $D \in \text{M}_n(\mathbb{Z}_p)$. By 6.6(i) and 6.2, $M\mathcal{B}$ (MB' , resp.) is an orthonormal basis of common eigenvectors for $\mathcal{C}\left(\begin{smallmatrix} I_n \\ 0 \end{smallmatrix}\right)$ ($\mathcal{C}\left(\begin{smallmatrix} 0 \\ I_n \end{smallmatrix}\right)$, resp.). Hence by 6.6(iii), the bases $M\mathcal{B}$ and MB' are mutually unbiased. Finally, since M is unitary, the bases \mathcal{B} and \mathcal{B}' are also mutually unbiased. \square

Thus we have shown, using our knowledge of the normalizer of $\mathcal{P}_{(p, \dots, p)}$, that having the system $(*)$, there are $p^n + 1$ mutually unbiased bases in the Hilbert space $\ell^2(\mathbb{Z}_{p^n})$, where p is a prime number. In the remaining part of this section we show how to generate these bases from the canonical one using one particular operator and an elementary commutative group of order p^n consisting of unitary diagonal matrices, i.e. $\cong \mathbb{Z}_p^n$.

First, recall a result by Wootters and Fields in [6] (mentioned also in [7]) that supports the existence of a system $(*)$:

Proposition 6.8. *There are symmetric matrices $B_1, \dots, B_n \in \text{M}_n(\mathbb{Z}_p)$ such that for every $0 \neq (\alpha_1, \dots, \alpha_n)^T \in \mathbb{Z}_p^n$ the matrix $\sum_{\ell=1}^n \alpha_\ell B_\ell$ is regular. In particular, let $\gamma_1, \dots, \gamma_n$ be a basis of the finite field \mathbb{F}_{p^n} as a vector space over the field \mathbb{Z}_p . Then any element $\gamma_i \gamma_j \in \mathbb{F}_{p^n}$ can be written uniquely as*

$$\gamma_i \gamma_j = \sum_{\ell=1}^n b_{ij}^\ell \gamma_\ell$$

where $b_{ij}^\ell \in \mathbb{Z}_p$. Now $(B_\ell)_{ij} = b_{ij}^\ell$ are the required matrices.

Now let \mathcal{D} denote the additive subgroup of $\text{M}_n(\mathbb{Z}_p)$ generated by B_1, \dots, B_n from 6.8. Clearly, $\mathcal{D} \cong \mathbb{Z}_p^n$ and it is easy to see that

$$\mathcal{H} := \left\{ \begin{pmatrix} I_n & B \\ 0 & I_n \end{pmatrix} \mid B \in \mathcal{D} \right\}$$

is a (multiplicative) commutative subgroup of $\text{Sp}_{2n}(\mathbb{Z}_p)$ that has a natural action (via matrix multiplication) on the set

$$\left\{ \begin{pmatrix} C \\ I_n \end{pmatrix} \mid C \in \mathcal{D} \right\}.$$

We consider now the system $(*)$ naturally as $\left\{ \begin{pmatrix} I_n \\ 0 \end{pmatrix} \right\} \cup \left\{ \begin{pmatrix} C \\ I_n \end{pmatrix} \mid C \in \mathcal{D} \right\}$ with the mappings

$$\begin{pmatrix} I_n \\ 0 \end{pmatrix} \xrightarrow{J'} \begin{pmatrix} 0 \\ I_n \end{pmatrix} \xrightarrow{\begin{pmatrix} I_n & A \\ 0 & I_n \end{pmatrix}} \begin{pmatrix} A \\ I_n \end{pmatrix} \xrightarrow{\begin{pmatrix} I_n & B-A \\ 0 & I_n \end{pmatrix}} \begin{pmatrix} B \\ I_n \end{pmatrix}.$$

Remark 6.9. The subspace of all symmetric matrices in $M_n(\mathbb{Z}_p)$ has a basis consisting of

- matrices E_{ij} , where $1 \leq i < j \leq n$, which have the entry 1 at the positions (i, j) and (j, i) and zeros otherwise, and
- matrices E_i , with $1 \leq i \leq n$ with the only non-zero entry 1 on the position (i, i) .

Now, put $F_i := I_{p^{i-1}} \otimes D_i \otimes I_{p^{n-i}}$ for $i = 1, \dots, n$. Using 5.6 and 5.7 we get that $\chi(\text{Ad}_{R_{ij}^{-1}}) = \begin{pmatrix} I_n & E_{ij} \\ 0 & I_n \end{pmatrix}$ and $\chi(\text{Ad}_{F_i}) = \begin{pmatrix} I_n & E_i \\ 0 & I_n \end{pmatrix}$. Thus taking unitary diagonal matrices in $\ell^2(\mathbb{Z}_{p^n})$,

$$K_\ell := \left(\prod_{i=1}^n F_i^{b_{ii}^\ell} \right) \left(\prod_{1 \leq i < j \leq n} R_{ij}^{-b_{ij}^\ell} \right) \in U_{p^n}(\mathbb{C})$$

for $\ell = 1, \dots, n$, we get

$$\chi(\text{Ad}_{K_\ell}) = \begin{pmatrix} I_n & B_\ell \\ 0 & I_n \end{pmatrix}$$

Let now \mathcal{K} denote the multiplicative subgroup of $\text{GL}_{p^n}(\mathbb{C})$ generated by K_1, \dots, K_n . We have an isomorphism $\mathcal{K} \rightarrow \mathcal{H} : K \mapsto \chi(\text{Ad}_K)$. Hence $\mathcal{K} \cong \mathbb{Z}_p^n$. We can now choose our set of $p^n + 1$ mutually unbiased bases in $\ell^2(\mathbb{Z}_{p^n})$ as

$$\{\mathcal{E}\} \cup \{KSE \mid K \in \mathcal{K}\}.$$

Indeed, by 6.2, 6.4 we have that \mathcal{E} , \mathcal{SE} and KSE are (in this order) orthonormal bases of common eigenvectors for $\mathcal{C}\left(\begin{smallmatrix} I_n \\ 0 \end{smallmatrix}\right)$, $\mathcal{C}\left(\begin{smallmatrix} 0 \\ I_n \end{smallmatrix}\right)$ and $\mathcal{C}\left(\begin{smallmatrix} A \\ I_n \end{smallmatrix}\right)$, where $\chi(\text{Ad}_K) = \begin{pmatrix} I_n & A \\ 0 & I_n \end{pmatrix}$. Now, by 6.7, these bases are mutually unbiased. The group \mathcal{K} acts on the system of bases as follows:

$$\mathcal{E} \xrightarrow{S} \mathcal{SE} \xrightarrow{K} KSE.$$

Remark 6.10. To have a better insight into the matrices S and K_1, \dots, K_n we will express the numbering of columns and rows as p -adic numbers, i.e. as n -tuples $\alpha_1 \dots \alpha_n$, with $\alpha_i \in \{0, \dots, p-1\}$, that correspond to $\alpha_1 p^{n-1} + \dots + \alpha_n p^0$. In this notation we get

$$S_{\alpha_1 \dots \alpha_n, \beta_1 \dots \beta_n} = \omega_p^{\sum_i \alpha_i \beta_i} / \sqrt{p^n},$$

$$(F_i)_{\alpha_1 \dots \alpha_n, \alpha_1 \dots \alpha_n} = \varepsilon^{-\alpha_i} \omega_p^{\binom{\alpha_i}{2}},$$

$$(R_{ij})_{\alpha_1 \dots \alpha_n, \alpha_1 \dots \alpha_n} = \omega_p^{\alpha_i \alpha_j},$$

and

$$(K_\ell)_{\alpha_1 \dots \alpha_n, \alpha_1 \dots \alpha_n} = \varepsilon^{-\sum_i b_{ii}^\ell \alpha_i} \cdot \omega_p^{\sum_i b_{ii}^\ell \binom{\alpha_i}{2} - \sum_{i < j} b_{ij}^\ell \alpha_i \alpha_j}$$

where $i, j, \ell = 1, \dots, n$, $i < j$ and $\varepsilon = \sqrt{-1}$ for $p = 2$ and $\varepsilon = 1$ otherwise.

7. Conclusions

In this paper we have described the symmetry groups of finite Heisenberg groups of arbitrary quantum systems consisting of a finite number k of subsystems with Hilbert spaces of finite dimensions n_1, \dots, n_k , thus extending our results obtained for bipartite systems [3]. For such a finitely composed quantum system the finite Heisenberg group is embedded in $\text{GL}_N(\mathbb{C})$, $N = n_1 \dots n_k$. It induces — via inner automorphisms Ad_M — an Abelian subgroup $\mathcal{P}_{(n_1, \dots, n_k)}$ in $\text{Int}(\text{GL}_N(\mathbb{C}))$. We have studied the normalizer of this Abelian subgroup in $\text{Int}(\text{GL}_N(\mathbb{C}))$ and have thoroughly described it. The obtained

symmetry group $\text{Sp}_{[n_1, \dots, n_k]}$ is the quotient group of the normalizer (theorem 5.9) and its further characterization was given in section 4.

The symmetry groups uncover deeper structure of FDQM. For instance, the cases when $n_1 = \dots = n_k = n$, $n \in \mathbb{Z}$, corresponding to dimensions $N = n^k$, are of particular interest. Then the symmetry group for a multipartite system with this special composition is $\text{Sp}_{[n, \dots, n]} \cong \text{Sp}_{2k}(\mathbb{Z}_n)$, which extends the bipartite case $\text{Sp}_4(\mathbb{Z}_n)$ considered in [3] and [14]. Thus our class of symmetry groups can be viewed as a very specific generalization of the familiar symplectic groups over modular rings [5].

We have exploited the cases when $n_1 = \dots = n_k = p$, p prime, corresponding to prime power dimension $N = p^k$, in section 6, where the symmetry group $\text{Sp}_{2k}(\mathbb{Z}_p)$ is applied to an alternative derivation of the maximal set of mutually unbiased bases in Hilbert spaces of prime power dimensions. Our group theoretic derivation uses the idea of [8], where a constructive existence proof for $k = 1$, $N = p$ prime, was based on consistent use of the symmetry group $\text{Sp}_2(\mathbb{Z}_p) \cong \text{SL}_2(\mathbb{Z}_p)$.

Our motivation to study symmetries of finite Heisenberg groups not in prime or prime power dimensions as in [18, 19, 21], but for arbitrary dimensions stems from our previous research where we obtained results not restricted to finite fields. Especially recall our paper [23] on Feynman's path integral and mutually unbiased bases. Also the recent paper [22] belongs to this direction, by dealing with quantum tomography over modular rings. The papers [25, 24] support our motivation, too, since they show that finite quantum mechanics with growing odd dimensions yields surprisingly good approximations of ordinary quantum mechanics on the real line. This suggests a promising subject of research to extend the results of [18, 20] on $\text{SL}_2(\mathbb{F}_q)$ from finite fields to modular rings.

Acknowledgements

The first author (M.K.) was supported by the project LC505 of Eduard Čech's Center for Algebra and Geometry. The second author (J.T.) acknowledges partial support by the Ministry of Education of Czech Republic, projects MSM6840770039 and LC06002.

References

- [1] Weyl H 1931 *The Theory of Groups and Quantum Mechanics* (New York: Dover) pp 272–280
- [2] Šťovíček P and Tolar J 1984 Quantum mechanics in a discrete space-time *Rep. Math. Phys.* **20** 157–170
- [3] Korbelař M, Tolar J 2010 Symmetries of the finite Heisenberg group for composite systems *J. Phys. A: Math. Theor.* **43** 375302 (15pp); arXiv: 1006.0328 [quant-ph]
- [4] Korbelař M, Tolar J 2012 Symmetries of finite Heisenberg groups for k-partite systems *J. Phys.: Conf. Ser.* **343** 012122; arXiv: 1201.3903 [math-ph]
- [5] O'Meara O T 1978 *Symplectic groups* (Providence RI: American Mathematical Society)
- [6] Wootters W K and Fields B D 1989 Optimal state-determination by mutually unbiased measurements *Ann. Phys. (N.Y.)* **191** 363–381
- [7] Bandyopadhyay S, Boykin P O, Roychowdhury V and Vatan F 2002 A new proof for the existence of mutually unbiased bases *Algorithmica* **34** 512–528; arXiv: quant-ph/0103162
- [8] Šulc P and Tolar J 2007 Group theoretical construction of mutually unbiased bases in Hilbert spaces of prime dimensions *J. Phys. A: Math. Theor.* **40** 15099–15111; arXiv: 0708.4114 [quant-ph]
- [9] Vourdas A 2004 Quantum systems with finite Hilbert space *Rep. Progr. Phys.* **67** 267–320
- [10] Kibler M R 2008 Variations on a theme of Heisenberg, Pauli and Weyl *J. Phys. A: Math. Theor.* **41** 375302
- [11] Wootters W K 1987 A Wigner-function formulation of finite-state quantum mechanics *Ann. Phys. (N.Y.)* **176** 1–21
- [12] Patera J and Zassenhaus H 1989 On Lie gradings I *Lin. Alg. Appl.* **112** 87–159
- [13] Havlíček M, Patera J, Pelantová E and Tolar J 2002 Automorphisms of the fine grading of $\text{sl}(n, \mathbb{C})$ associated with the generalized Pauli matrices *J. Math. Phys.* **43** 1083–1094; arXiv: math-ph/0311015
- [14] Pelantová E, Svobodová M and Tremblay J 2006 Fine grading of $\text{sl}(p^2, \mathbb{C})$ generated by tensor product of generalized Pauli matrices and its symmetries *J. Math. Phys.* **47** 013512

- [15] Han G 2010 The symmetries of the fine gradings of $\mathfrak{sl}(n^k, \mathbb{C})$ associated with direct product of Pauli groups *J. Math. Phys.* **51** 092104 (15 pages)
- [16] Schwinger J 1960 Unitary operator bases *Proc. Nat. Acad. Sci. U.S.A.* **46** 570–579, 1401–1415
- [17] Folland G B 1989 *Harmonic Analysis on Phase Space* (Princeton, NJ: Princeton University Press)
- [18] Balian R and Itzykson C 1986 Observations sur la mécanique quantique finie *C. R. Acad. Sci. Paris* **303** Série I, n. 16, 773–777
- [19] Vourdas A 2007 Quantum systems with finite Hilbert space: Galois fields in quantum mechanics *J. Phys. A: Math. Theor.* **40** R285–R331
- [20] Neuhauser M 2002 An explicit construction of the metaplectic representation over a finite field *Journal of Lie Theory* **12** 15–30
- [21] Gibbons K S, Hoffman M J and Wootters W K 2004 Discrete phase space based on finite fields *Phys. Rev. A* **70** 062101 (23 pp)
- [22] Vourdas A and Banderier C 2010 Symplectic transformations and quantum tomography in finite quantum systems *J. Phys. A: Math. Theor.* **43** 042001 (9pp)
- [23] Tolar J and Chadzitaskos G 2009 Feynman’s path integral and mutually unbiased bases *J. Phys. A: Math. Theor.* **42** 245306 (11pp)
- [24] Digernes T, Husstad E and Varadarajan V S 1999 Finite approximation of Weyl systems *Math. Scand.* **84** 261–283
- [25] Digernes T, Varadarajan V S and Varadhan S R S 1994 Finite approximations to quantum systems *Rev. Math. Phys.* **6** 621–648